National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

The NSA/IAD National Security Cyber Assistance Program (NSCAP) Cyber Incident Response Assistance (CIRA) Accreditation Instruction Manual

An overview of the NSCAP CIRA Accreditation:

Requirements for Intrusion Detection, Incident Analysis and Response

Program Release Version 3.1

Date: 06 January 2015

Table of Contents

1 Introduction 5
1.1 Fees and Charges 6
1.2 Application Submittals 6
2 Qualifications 7
3 CIRA Services – The Accreditation Process 8
3.1 Overview 8
3.2 Application Submittal 8
3.3 How New Applications Are Scored 8
3.4 Issuing an Accreditation 9
4 Accreditation Maintenance 9
4.1 Changes in Status 9
4.2 Accreditation Renewals 10
4.3 Renewal Application Scoring 11
5 Non-Accredited Packages 12
6 Accreditation Application Package Contents 12
6.1 Business Statement of Intent 13
6.2 Core Capabilities Overview 13
6.3 Processes and Procedures 14
6.4 CIRA Key Team Qualifications Report 15
6.5 CIRA Education and Training Plan 15
6.6 Past Performance 15
6.7 Client-Furnished Information and Data Management Plan 16
References 18
Appendix A - Process and Procedure Guide 19
1 Introduction 19
2 Preparation and Planning (Pre-Deployment) 20
2.1 Elements of a CIRA Services Agreement 21
2.2 Client Engagement Management 22
2.3 Communication Management 23
2.4 Preliminary Data Collection 23

2.5 Engagement Tools and Resources 24
2.6 Travel Management 25
2.7 Rules of Engagement 25
3 Incident Identification, Intrusion Detection, and Analysis (Investigation) 25
3.1 Log Collection and Analysis 26
3.2 Network Traffic Data Collection and Analysis 27
3.3 Host Integrity Data Collection and Analysis 28
3.4 Incident Analysis 30
4 Containment and Remediation Recommendations 32
5 Post-Incident Analysis and Final Report 34
6 Lessons Learned 35
Appendix B – CIRA Key Team Qualifications Guide 37
1 Introduction 37
Appendix C – Accreditation Application Package 0
1 Application for Accreditation 1
2 Business Statement of Intent Certification 2
3 CIRA Key Team Qualifications Report * 3
4 Application Content Checklist for a Candidate Organization 4

List of Tables

Table 1: Application Scoring 9
Table 2: Components of an NSA/IAD CIRA Accreditation Application Package 12
Table 3: CIRA Key Team Qualifications Guidance 39
Table 4: DOD Approved Baseline Certifications 43
Table 5: Accreditation Reference Table 44

NOTICE

This version of the CIRA Accreditation Instruction Manual (Version 3.1) contains requirements and expectations that are materially the same as those identified within Version 3.0 of the manual that was used under the 6 August 2014 open call for applications. Accreditations issued under Version 3.0 shall apply equally to Version 3.1 of the manual. Companies accredited under Version 3.0 must follow the procedures identified herein to renew their accreditation. Version 3.1 is the updated version of 3.0 and consists of the following changes: Reformatted Table 2, section 6 page 15 so as to reflect EXACT content needed for submittal using the web site portal as the guide; changed accreditation period from 12 to 24 months; reworded the press release instructions found in Section 1.5; added Reference page to include germane referenced publications; changed Business Statement of Intent signatory requirement for two executives to sign the statement; added clarification of PII in section 1.2 and 4.2 and expanded Intrusion Detection elements in Appendix B, Section 3.1.C.

1 Introduction

A. The National Security Agency/Information Assurance Directorate (**NSA/IAD) National Security Cyber Assistance Program (NSCAP) Cyber Incident Response Assistance[1] (CIRA)** accreditation was designed to meet the growing needs of the U.S. Government, supplementing the incident response and intrusion detection services that NSA/IAD provides to the Department of Defense (DOD), Intelligence Community (IC), and other organizations as authorized and directed. The core objective of CIRA accreditation is to identify companies qualified to provide rapid, on-site support to National Security Systems (NSS) owners and operators in incident response and intrusion detection. Broadly speaking, assessment of capabilities is based on the provider's ability to:

1. Consistently deliver CIRA services using thoroughly documented, repeatable processes and procedures.
2. Assign highly skilled and qualified staff who are eligible to hold U.S. Government security clearances to follow the aforementioned processes and procedures to deliver CIRA services.
3. Maintain and improve the quality of delivered services through training initiatives, improvement of analytical capabilities, and use of lessons learned from previous deployments or engagements to refine their processes.
4. Provide past performance examples of its successful delivery of these services.

B. CIRA accreditation is awarded to qualified CIRA service providers who are capable of providing comprehensive, high quality and repeatable CIRA services to operators of classified and unclassified NSS[2]. Accreditation is awarded based upon NSA/IAD's review and positive comparison of a candidate organization's application package to the criteria identified in Appendix A of this document.

C. Candidate organizations are reminded that applications are not to be structured as a response to a request for information or a request for proposal. The application process is not modeled after those processes nor is it intended to meet those types of objectives.

D. For the NSA/IAD to understand the capabilities of a candidate organization they must provide a high level of assurance that they know how to deliver CIRA services in a consistent and

[1] Cyber Incident Response Assistance is an identified capability under NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, Incident Response Family of Controls, IR-7 Incident Response Assistance (reference b.)

[2] "All U.S. Government classified networks have been designated as NSS. The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or contractor of an agency, or other organization on behalf of an agency (i) the function, operation, or use of which (I) involves intelligence activities; (II) involves Cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (v) subject to paragraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (i)(V), above, does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). DoD has also designated the Non-Secure Internet Protocol Router Network (NIPRNet) as a NSS. *See* 44 U.S.C. § 3542(b)(2), for the complete definition of "NSS.""

repeatable manner. One of the few ways that these capabilities can be conveyed to an evaluator is through the submission of documented processes and procedures that are used by the candidate organization on a regular basis. The Government recognizes that incident response processes and procedures can never address every variable and, at some point, each engagement transitions to reliance on the skills of the CIRA team. However, the basics of a CIRA service engagement, including preparation and planning, assigning the right staff based on engagement needs, selecting the right tool sets, coordinating travel and communication, pre-deployment and post deployment information collection, information analysis, client reporting and performance improvement, are all consistent and repeatable activities. For the NSA's CIRA accreditation to be awarded, these activities are expected to be documented as processes and procedures and included in the application package. Each process and procedure may be supplemented with a narrative that provides an overview of when and why each process is used. However, narratives on their own may not replace the documented processes and procedures in an application package.

E. Please note: The content and structure comprising a candidate organization's processes and procedures is the primary information on which NSCAP evaluators assess and score the application package. If a process or procedure is not thoroughly documented in the application package, the NSA/IAD must assume that it cannot be executed in a consistent and repeatable manner thereby leading to inconsistent results and levels of performance between CIRA engagements. Additional guidance with respect to the level of detail each process and procedure should contain may be found in section 6.3, 'Processes and Procedures', of this manual.

1.1 Fees and Charges

A. Candidate organizations **are not charged a fee** for any portion of the accreditation or the evaluation process at this time. This includes, but is not limited to, NSA/IAD's receipt of the application, its review and evaluation, the generation of any questions, the evaluation of answers associated with those questions, rejection or acceptance of an application for accreditation, the actual accreditation response or its subsequent record maintenance by NSA/IAD for the accreditation period. Additionally, NSA/IAD **will not provide funding** for any portion of a candidate organization's costs associated with the accreditation process or its subsequent accreditation maintenance. This includes, but is not limited to, the organizational costs to prepare any portion of the application or application package content, the preparation of responses to questions generated during NSA/IAD's review of the application package contents, or the subsequent updates of the application package for resubmittal, the receipt of the accreditation, or notifying NSA/IAD of changes in the candidate organization's status during the accreditation period once an accreditation is issued.

1.2 Application Submittals

A. By submitting an application for CIRA accreditation, hereafter referred to as application package, the candidate organization is representing that the information provided within their application package is correct and accurate to the best of the submitter's knowledge. The candidate organization is responsible for ensuring that all personally identifiable information (PII) data is removed from or redacted in the application package prior to submittal. A candidate

organization's participation in any portion of the accreditation process outlined herein constitutes recognition and acceptance of these conditions.

B. The submittal of an application package by a candidate organization does not ensure CIRA accreditation. Further, CIRA accreditation does not automatically lead to the issuance of a U.S. Government security clearance by NSA/IAD or other branch of the Federal Government.

C. Application package content or material received that is labeled as "Company Proprietary", "Company Confidential", or similar markings will be identified by the Government as Contractor PROPIN. Application packages received by NSA/IAD will be processed and handled in a manner that provides a reasonable level of assurance that any Contractor PROPIN is protected from unauthorized access or disclosure within NSA/IAD. The Government retains contractor personnel to provide support to this program. These contractors have signed non-disclosure agreements with NSA/IAD to prohibit the unauthorized access or disclosure of Contractor PROPIN. Submission of an application package by a candidate organization constitutes acknowledgement and acceptance of NSA/IAD's use of contractor personnel for NSCAP support. Questions concerning the roles of contractors as part of this program should be directed to NSCAP@nsa.gov.

D. It is anticipated that, in many instances, incident response support to NSS owners/operators can only be performed at the NSS owners/operators' facilities and that the delivery of remote incident response services (i.e., delivering the incident response services from the service providers own facilities) will not be possible in a timely manner. This accreditation is intended to identify organizations that can support all NSS owners and operators within the facilities where the NSS is located. Managed Security Service Providers that offer only remote access-based incident response services, or organizations that operate incident response services for only their internal organization, or only provide incident response services to internally hosted systems for their clients (i.e. outsourcing and system hosting services, etc.) are service offerings that are not within the scope of this accreditation.

E. This accreditation is awarded to qualified service providers that deliver *on-site* (i.e. on the client's work site and within their physical facilities) intrusion detection and incident response services. These on-site providers deliver services that include, but are not limited to, intrusion detection, malware analysis and reverse engineering, forensics, packet capture (PCAP) used to perform network traffic analysis (IPv4 and IPv6), host integrity checking, containment, eradication, remediation and ongoing mitigation recommendations to their clients.

F. Once approved, the NSA/IAD CIRA accreditation is valid for 24 months.

2 Qualifications

A. To qualify for this accreditation, the candidate organization must offer CIRA services as a core part of its business model. These services must be offered in a manner that is consistent with the following guidelines. The candidate organization:

1. Provides CIRA services under agreement to Industry[3] and/or Government CIRA service consumers.
2. Provides agreement-based services that include:
    a. Deploying CIRA teams that provide on-site cyber intrusion detection and incident response analysis and support
    b. Providing containment and remediation recommendations and assistance
    c. Post-incident/lessons learned reports and plans
3. Assumes responsibility for the delivery of products, reports and other deliverable items to the extent agreed to within its service agreements.
4. Has CIRA Team staff members who are eligible to receive a U.S. Government security clearance.
    a. Candidate organizations are not required to have a facility clearance or employ cleared individuals to apply for and receive accreditation.

3 CIRA Services – The Accreditation Process

3.1 Overview

A. The Government's goal is to complete the accreditation process within 60 calendar days after the start of the evaluation process once a complete application package from a candidate organization is received.

3.2 Application Submittal

A. The candidate organization will assemble its application package, ensuring that it contains a complete set of supporting information in accordance with the instruction manual. The completed sections of the package will then be uploaded for review via the NSCAP Application Portal located on the IAD.gov web page at the following link: https://www.iad.gov/CIRA/index.cfm

3.3 How New Applications Are Scored

A. NSA/IAD will evaluate each component of the application package in accordance with evaluation guidelines documented within each of the appendices contained herein. Component scoring weights were developed based on the importance of a capability to NSA/IAD in support of NSS incident response assistance.

B. The CIRA accreditation program will work with each candidate organization to clarify the content of its application package as part of the 60 day application processing schedule. During the first 50 calendar days of this period, and at the discretion of the evaluators, a candidate organization may be asked for clarification of any portion of the material provided within their application package. As appropriate, a candidate organization receiving questions will be allowed to provide verbal clarifications, written updates, modifications or replacements to the parts of its original application submittal that were questioned. For each question, a due date will be negotiated. It is expected that responses to all questions will be received by the evaluator within the first 50 days of the processing period and the application package will be considered to be final at that point. The final 10 days of the 60 day application period is

[3] Industry, as used herein, includes all non-Governmental organizations

allocated to conducting reviews, applying final scores, and completing the application processing.

C. NSA/IAD NSCAP evaluators will score each part of the final application using one of three values from Table 1 below:

Table 1: Application Scoring

If ...	Then ...
1. The representations and supporting information are compliant with the instructions provided in Appendix A, ...	**1.** It is scored at 100% of its assigned value.
2. It is substantially compliant but not complete (after the Q&A process is completed), ...	**2.** It is scored at 70% of its assigned value.
3. A required item is not substantially complete or simply missing, ...	**3.** It is scored at 0%.

Candidate organizations scoring at or above a combined score of 85% become eligible for accreditation if all other application requirements are met.

3.4 Issuing an Accreditation

A. The NSA/IAD NSCAP Office will make the final decision regarding the accreditation of the candidate organization. A Government representative, authorized by NSA/IAD Executive Management, will send a letter to the designated Point of Contact (POC) from the candidate organization with the NSCAP Office's decision. Accreditations are valid for a period of 24 months from the date on the accreditation letter and will apply only to the instruction manual that is in place at the time of accreditation award.

Please note: Each accredited organization is required to submit any of its marketing materials identifying the National Security Agency, the National Security Cyber Assistance Program, the Cyber Incident Response Assistance Accreditation, associated acronyms, or other Agency references to the NSCAP Program Office for its prior written approval. All such materials must be submitted to NSCAP@nsa.gov at least 30 days prior to their proposed distribution in order to obtain the Agency's written approval.

4 Accreditation Maintenance

A. Accreditation maintenance addresses requirements to notify NSA/IAD NSCAP Office of any material or significant changes to the accredited organization's status during the accreditation period and the renewal of the accreditation at the end of the accreditation period.

4.1 Changes in Status

A. During the renewal accreditation period, the accredited organization is required to report any material or significant changes to its status within 30 days of its occurrence. Material or significant changes are those that may affect the accredited organization's ability to continue to deliver CIRA services to NSS owners and operators.

B. Such changes may include, but are not limited to, changes in the organization and/or its staff that result in its ineligibility to hold a U.S. Government clearance, changes in corporate ownership including significant foreign/non-U.S. investments into the organization, and changes in the organization's focus on CIRA service delivery. Such material and significant changes may result in a reexamination and/or revocation of the accreditation by NSA/IAD.

C. Changes in staff or key team members that are consistent with normal employee turnover or attrition rates, updates to policies and procedures, or other normal changes to an organization's operational posture are not considered material or significant and do not need to be reported to NSA/IAD prior to accreditation renewal.

4.2 Accreditation Renewals

A. Renewals are not automatic. If an accredited organization wishes to renew its accreditation, it must submit its renewal application to NSA/IAD no later than 30 days before the end of the accreditation period. Accredited organizations **are not** charged any fee to apply for a renewal and NSA/IAD **will not provide funding** for any aspect of the renewal process.

B. As the CIRA Accreditation Instruction Manual is updated and modified over time, accredited organizations may need to update and resubmit certain elements of their accreditation package to remain current with the new version of the manual. NSA/IAD will identify areas where mandatory updates are required at the time each update is issued under the NOTICE section, page 7, of the manual.

C. Accredited organizations will be eligible to renew their accreditations 30 days prior to the end of the 24 month accreditation period. Renewals are voluntary, but require the timely submission of a renewal application package to be submitted to NSA/IAD through the application process. An organization's existing accreditation will remain in effect until NSA/IAD completes its evaluation of the renewal application package and provides notice to the organization of the acceptability of their submittal as a basis for renewal.

D. The renewal accreditations will also be valid for a period of 24 months from the date on the accreditation letter and will apply only to the instruction manual version that is in place at the time of accreditation award.

E. The renewal application package must include the following:

1. It is required that the accredited organization provide confirmation that providing CIRA services remains a focus of their business model. The statement must be signed by two executive officers from the accredited organization who have the authority to make this level of commitment.
2. It is required that the accredited organization provide past performance reports in the format required in Section 6.6 - Past Performance, covering any additional work performed during the previous 24 months. NSA/IAD expects that the accredited organization will have performed at least two CIRA service engagements during that reporting period. Any NSS CIRA service engagement that was performed during the period of past performance should be included as part of the renewal application package.

3. If applicable, the accredited organization must report and provide copies of any updates, enhancements or replacements to their processes and procedures that were changed from those accepted as part of their initial accreditation or accepted in subsequent renewal submittals.
4. If applicable, the accredited organization must report staffing changes to its Key Team Members and provide an updated CIRA Key Team Qualifications Report as part of its renewal application package.
5. The previously accredited organization is responsible for identifying and complying with all accreditation requirements included in the version of the manual posted at the time of their renewal application. If applicable, the accredited organization must report and submit any other changes to any components that were originally contained in the application package or in subsequent renewal application packages, or to make their renewal package compliant with the current version of the manual that is in use at the time of application for accreditation renewal.

F. If no changes were made to the documents identified in items 3-5 within this list during the renewal period, the accredited organization must provide a statement to NSA/IAD with their renewal submittal that no changes were made.

G. The accredited organization will assemble the appropriate content for inclusion in the renewal application package and provide the package to NSA/IAD through the submittal process. All content provided as part of this renewal application package must be identified as renewal content. PII data should be removed or redacted from all portions of the renewal application package. After NSA/IAD NSCAP evaluators receive the completed renewal application package from an accredited organization, their goal is to complete the renewal process within 30 days.

4.3 Renewal Application Scoring

A. The renewal application package content will be evaluated, and each new or changed component will be scored, using the same approach described in the original evaluation process. That score will replace the previous score for the new or changed component. The total score, combining the old and the new content scores, must result in a score at or above the 85% threshold to become eligible for accreditation renewal.

B. NSA/IAD NSCAP evaluators are authorized to work with accredited organizations to clarify the content of the renewal application packages. Clarification activities will not be permitted to impact the 30 day renewal application package evaluation period. Failure of an accredited organization to provide timely and/or concise responses to clarification requests will result in the information in the possession of NSA/IAD to be scored as received. All content in each renewal application package, including any supplemental information provided through the clarification process, will be scored. Scoring will be performed using the same approach as in the original accreditation process.

C. The NSA/IAD Program Office makes the final decision regarding the accreditation renewals of the previously accredited organizations. The program office will send a letter to the designated POC from the accredited organization with its decision.

5 Non-Accredited Packages

A. If a candidate organization's application is scored below 85%, CIRA accreditation will not be issued. Notification of non-accreditation will be by letter to the candidate organization's assigned POC accompanied with a summary of application deficiencies. The candidate organization may then reapply after 90 days.

6 Accreditation Application Package Contents

A. NSA/IAD has implemented appropriate controls to manage access to any data that it receives as part of an application package from a candidate organization. It will consider all data submitted as part of an application package as proprietary to the candidate organization and will be handled accordingly.

B. All organizations applying for the NSA/IAD CIRA accreditation must submit an application package to NSA/IAD containing the following information:

Table 2: Components of an NSA/IAD CIRA Accreditation Application Package

Focus Area	Description
Business Statement of Intent	A formal statement by the candidate organization asserting its commitment to perform CIRA services. The statement must be signed by two executive officers of the organization that have the authority to make this level of commitment.
Core Capabilities Overview	An overview of the baseline processes that the candidate organization uses to conduct CIRA services, including descriptions of the tactics and techniques used to deliver those capabilities. White papers or technical capabilities documents used for marketing may be acceptable to meet this requirement.
Processes and Procedures	Processes and procedures, aka Tactics, Techniques and Procedures (TTPs), used to perform and deliver CIRA services including, but not limited to, intrusion detection, malware analysis and reverse engineering, forensics, PCAP and network traffic analysis for IPv4 and IPv6, host integrity checking, containment, eradication, remediation and ongoing mitigation.
CIRA Key Team Qualifications Report	Documentation that identifies and describes the skills of the candidate organization's Key Team Members who will deliver CIRA services to its clients. Skills should correspond with the guidance in Appendix B - CIRA Key Team Qualifications Guide. The personally identifiable information may be redacted[4].
CIRA Education and Training Plan	Provide a formal training plan that the candidate organization uses to ensure that the technical and management staff are kept up-to-

[4] (Black's Law Dictionary): A document where confidential or sensitive information has been removed. In this case it is to mean "non-attributable" to the client.

Focus Area	Description
	date on the organization's CIRA processes, procedures, techniques, and on the tools used to support CIRA service delivery.
Past Performance	Provide at least three (3) redacted final reports, modified to protect the client's identities, generated at the conclusion of separate CIRA service engagements, and performed by the candidate organization within the past 24 months. To the extent possible, these reports should reflect the use of the processes and procedures provided as part of the application package to confirm their use as part of the service delivery process.
Client-Furnished Information and Data Management	Provide plans and processes that are used to manage customer property and/or information obtained during a CIRA engagement[5].

6.1 Business Statement of Intent

A. The candidate organization must prepare and submit a formal statement to NSA/IAD certifying that it:
   1. Believes it is eligible[6] to hold a U.S. Government security clearance.
   2. Currently intends to maintain its capabilities for delivering CIRA services as represented in its application package for the period of the accreditation (24 months).
   3. Plans to notify the NSA/IAD accrediting office of any material changes to its status. These include, but are not limited to, changes in organization ownership or reporting responsibility, changes to its business focus, changes in clearance eligibility, etc.

B. The statement must be signed and dated by two executive officers of the organization that have the authority to make this level of commitment.
C. A template for this formal statement may be found in **Appendix C – Accreditation Application Package**.

6.2 Core Capabilities Overview

A. The candidate organization must prepare and submit an overview of its core incident response capabilities to NSA/IAD. The overview should include baseline processes that the candidate organization uses to conduct CIRA services. This should include descriptions of the tactics and techniques used to deliver those capabilities. Candidate organizations may provide this overview or narrative in a format they are already using. It must be separately marked as the "[candidate organization name] Core Capabilities Overview"

[5] This plan may include, but is not limited, to the handling of collected logs, traffic data and collected hard drives that will be subjected to forensic analysis. Though not required for accreditation, this plan may be supplemented by identifying how the organization handles and manages US Government classified information or material.

[6] The need of a CIRA service provider to receive classified data, or to possess a certain security clearance will be determined by the National Security Systems (NSS) owner or operator and the scope of the specific engagement, program and agency being supported. Please note that representations to eligibility do not equate to a commitment on the part of the NSA/IAD to sponsor a candidate organization for a security clearance.

6.3 Processes and Procedures

A. The candidate organization must prepare and submit the processes and procedures that it currently uses to deliver CIRA services to NSA/IAD. It is expected that as part of the application package, the candidate organization will include processes and procedures that are currently in use by the candidate organization in the performance of their CIRA business activities and that each is ***discreet, unique and unambiguous***.

B. A submitted process or procedure that has been co-mingled or structured so that it addresses multiple capabilities is not desired. Each capability is scored discreetly and, therefore, must be presented discretely.

C. NSA/IAD requests that each individual process and procedure that is submitted as part of the application package includes the following elements in an easily identifiable format[7]:
   1. The identification of personnel/staff (by job category, labor category, and/or position) that are responsible for performing or completing the process/procedure.
   2. The identification of inputs, (from previously started or completed process/procedure) whose outputs are required to begin or complete the subject process/procedure. These are items that are acted upon by the subject process/procedure and used or transformed to create its outputs.
   3. The identification of controls that establish the bounds of the subject process/procedure, including instructions contained in the process/procedure itself, the Engagement Agreement, associated legal constraints, and/or other factors that the candidate organization considers important.
   4. Process enablers to include tools, resources, or technologies that are required to perform the subject process/procedure to obtain the desired results.

D. These documents must be compliant with the capabilities set forth in **Appendix A - CIRA Processes and Procedures Guide.**

E. The general areas of system component focus for Cyber Incident Response are for log analysis, network traffic analysis and host integrity verification and validation. These processes may include, but are not limited to, instruction on the collection, aggregation and normalization, and analytical use of collected data. Since each CIRA services engagement is different, the processes should reflect a balanced approach in their applicability.

F. The processes and procedures may be provided in the candidate organization's format. Each process or procedure must be separately marked as the "[candidate organization name] [Process or Procedure Name]." The names of the candidate organization's processes and procedures submitted as part of the application package should be cross-referenced with the naming conventions in **Appendix A**.

[7] INCOSE Systems Engineering Handbook v. 3.2.2, INCOSE-TP-2003-002-03.2.2, October 2011 (reference j) or ISO/IEC 15288:2008 are considered structurally sound. Other approaches are equally acceptable and may be more appropriate for the candidate organization's business model.

6.4 CIRA Key Team Qualifications Report

A. The candidate organization must identify five Key Team Members who support its incident response service offering as part of its application package. Each Key Team Member identified must be a full-time employee of the candidate organization and whose primary job function is the support or delivery of incident response services. Each Key Team Member may only be associated with one of the key positions identified within **Appendix B - CIRA Key Team Qualifications Guide.** That individual must have the skills qualifying him or her for that position. The candidate organization must complete the form titled **CIRA Key Team Qualifications Report** that is found in **Appendix C, Item 3** of this manual and associate each Key Team Member with a specific position on that form. The completed Report must be submitted as part of the candidate organization's application package.

B. The candidate organization is not required nor expected to assign all five Key Team Members to each engagement, but is expected to have the five Key Team Members reasonably available to participate in or support any engagement within the terms of the Organization's engagement agreement. It is expected that any deployment team will be supplemented with additional individuals, as needed, to meet the obligations and commitments made within individual engagement agreements.

6.5 CIRA Education and Training Plan

A. The candidate organization must submit an Education and Training Plan to NSA/IAD that describes how it ensures that its CIRA Service employees have on-going education and training to address emerging technologies and threats. This may include the following:

1. Formal technical training
2. Briefings from product vendors
3. Community forums, conferences, symposiums, technical exchanges, etc.
4. Participation in cyber incident response exercises
5. Government or industry presentations on vulnerability exploits, threat mitigations, or similar CIRA service activities
6. A controlled technical environment used for hands-on training (and to evaluate new capabilities as appropriate)

B. This plan may be provided in the candidate organization's format and must be separately marked as the "[candidate organization name] Education and Training Plan."

6.6 Past Performance

A. The candidate organization must submit documentation to NSA/IAD to confirm that it:

1. Operates at least one CIRA Service Team
2. Has performed three (3) or more CIRA service engagements for its clients within 24 months prior to submitting the accreditation application package

B. The documentation should also identify the following:

1. **Engagement Overview**
   The candidate organization should describe:

a. How the work was initiated
b. The scope of the team's responsibility as defined within the agreement – the work that they performed (e.g., Leadership, Computer Network Defense (CND), Forensics, Auditing, Remediation, etc.)
c. How the engagement was managed
d. How the team's performance was measured

2. **Steps the candidate organization has taken to perform the work identified in the agreement and its subsequent modifications (as applicable). It should also describe:**
   a. How the incident was investigated and how specific methodologies and tactics were used
   b. What data was collected, how it was collected, and what analysis was performed on it
   c. Key events within the engagement that led to its success
3. **Redacted portions of working papers (if available).**
   a. This confirms that processes and procedures were followed, and that those processes and procedures, when followed, generated the sought-after data or information.
   b. These also identify the team's level of activity in delivering the CIRA services.

5. **Redacted final reports that provide appropriate details of the delivered services.**

6. **Description of how the integrity of the network was restored and maintained, if applicable.**

C. NSA/IAD does not wish to receive any data that is considered 3rd party proprietary or confidential (i.e., a candidate organization's client's data). This type of data is commonly found in incident response summary reports and samples of collected system or network data. Any 3rd party data should be hidden or removed if it is part of a past performance report.

D. This Past Performance data may be provided in the candidate organization's format. It must be separately marked as the "[candidate organization name] Past Performance Report number ["1", "2", "3", etc.]."

6.7 Client-Furnished Information and Data Management Plan

A. The candidate organization must submit an Information and Data Management Plan to NSA/IAD as part of its overall application package. The candidate organization must be able to securely receive from its clients and then effectively manage data, information, material and/or software applications, while ensuring that the confidentiality, availability and integrity of each item received is maintained. These items may be obtained during the data collection process or provided by or through the client to support the data collection process. This plan should include processes to address data collection, data transport and data at rest protections, and client record and information retention and protection. These processes should describe:

1. How the candidate organization receives and tracks client-furnished data, information, material and/or software applications
2. How it tracks and manages property receipts and its general property protection processes once those items are in their care

3. If consistent with its business model, the candidate organization's property management processes must address the receipt, management and disposition of classified data

B. This client-furnished document may be provided in the candidate organization's format. It must be separately marked as the "[candidate organization name] Client-Furnished Information and Data Management Plan".

References

The following documents are referenced or provide amplifying or supplementary information. Future updates to referenced documents will be considered applicable to this instruction manual.

a) National Institute of Standards and Technology (NIST) Special Publication 800- 37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, revised February 2010.

b) National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013,*Incident Response Control Family, Incident Response Assistance* (IR-7).

c) National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*, (August 2012).

d) National Institute of Standards and Technology (NIST) Special Publication 800-86, *Guide to Implementing Forensic Techniques Into Incident Response*, (August 2006).

e) Committee on National Security System Policy No.22, *Policy for Information Assurance Risk Management for National Security Systems,* January 2012.

f) Committee on National Security System Directive 502, *National Directive on National Security Systems*, 16 December 2004.

g) Committee on National Security System Instruction No. 1010, *24 x 7 Computer Incident Response Capability (CIRC) on National Security Systems*, revised 03 October 2012.

h) Committee on National Security System Instruction No.1253, *Security Categorization and Control Selection for National Security Systems*, 27 March 2014. *Incident Response Control Family, Incident Response Assistance* (IR-7)

i) DOD Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management*, updated April 2007

j) International Council on Systems Engineering (INCOSE) *Systems Engineering Handboo*k v. 3.2.2 INCOSE-TP-2003-002-03.2.2, October 2011

Appendix A - Process and Procedure Guide

1 Introduction

A. The **NSA/IAD Cyber Incident Response Assistance (CIRA)** accreditation is provided to organizations that meet the accreditation capabilities as defined within this Appendix and as reflected in the policies and procedures they will submit as part of their application.

B. A candidate organization's capabilities, as identified within its processes and procedures aka Tactics, Techniques and Procedures (TTPs), the represented skills of its CIRA Services Team, and its past performance are all key evaluation factors considered as part of the accreditation evaluation process.

C. NSA/IAD expects that the policies and procedures provided by candidate organizations will be structured as generic documents and that those documents will address, at some level, the capabilities as described in this Appendix. NSA/IAD presumes that the candidate organization has developed guidance that meets its own needs, having balanced the content of its processes and procedures between being technically detailed or technically limited (high level) against the skills of the staff that it hires and retains for delivering those incident response assistance services.

D. For application evaluation purposes, NSA/IAD will examine the content of the documents to ensure that all elements of the capabilities are addressed at some level, and for the level of sufficiency in meeting capabilities objectives. NSA/IAD will then balance the results against the types and skill levels of those individuals identified as the service providers as part of the **Appendix B - CIRA Key Team Qualifications Guide.**

E. Specifically, NSA/IAD expects that highly detailed processes and procedures can be performed by competent individuals with a basic understanding of the technical and managerial aspects of incident response. Conversely, high-level processes and procedures that lack detail usually require individuals with greater incident response expertise to ensure adequate performance of the CIRA service delivery work.

F. The balance between processes and procedures and employee skills is made at the discretion of the candidate organization. NSA/IAD will expect that a reasonable balance between the two will be demonstrated through the data in the candidate organization's application package. The success of a candidate organization in maintaining its represented CIRA service delivery model is reflected in the success of its business model, represented by its past performance submittals.

G. The sections of this Appendix summarize and guide candidate organizations on what NSA/IAD expects to be included in their processes and procedures before they are submitted for evaluation.

H. This Appendix is structured so that each section includes both Capabilities and Potential Documentation Content. These are defined as:

1. ***Capability***: A candidate organization **must** demonstrate how it intends to comply with criteria defining a specific capability. The candidate organization's processes and procedures should show, at a minimum, who is responsible for, and how a specific capability will be delivered.

2. ***Potential Documentation Content***: A candidate organization is expected to provide its approaches to meeting the standard capabilities. Consequently, each process and procedure section describes and clarifies the type of content that a candidate organization could include in its documentation. It does not represent a required model of what must be included in the process or procedure. It is only listed to show possibilities for inclusion.

3. NSA/IAD seeks a set of documents that demonstrates compliance with the instructions and criteria contained within this application manual. It is expected that each element identified within this Appendix and included as part of the candidate organization's application package will consist of discreet, unique and unambiguous content that is currently in use by the candidate organization in the performance of its business activities and that directly addresses each separate capability identified herein. This section describes and clarifies the type of content that a candidate organization should include in its documentation.

I. NSA/IAD requests that each individual process and procedure submitted as part of the application package include the following elements:

   1. The identification of personnel/staff (by job category, labor category, and/or position) who are responsible for performing or completing the process/procedure
   2. Process inputs or items that are acted upon by the process and used or transformed to create the process outputs
   3. Process controls that establish the bounds of the process/procedure to include instructions contained in the process/procedure itself, the Engagement Agreement, and legal constraints
   4. Process enablers[8] to include tools, resources, or technologies that are required to perform the subject process/procedure

J. Should questions arise concerning a submitted process/procedure, the questions will be researched internally by the NSA/IAD evaluators. Should clarification from the candidate organization be required, the evaluation team will attempt to obtain the needed clarification from the candidate organization. However, completeness of the process/procedure s submitted will minimize delays in completing the evaluation.

2 Preparation and Planning (Pre-Deployment)

A. The initial phase of any engagement is to identify and document the CIRA Services Agreement. A candidate organization must establish a contractual or similar relationship (e.g., Agreement)

[8] INCOSE Systems Engineering Handbook v. 3.2.2, INCOSE-TP-2003-002-03.2.2, October 2011 (reference j) or ISO/IEC 15288:2008 are considered to be acceptable structural approaches though others are acceptable and may be more appropriate for the candidate organization's business model.

with its client to deliver CIRA services. It is assumed that the agreement's supporting business and administrative relationships will be established and negotiated between the candidate organization and its client. The structure of that agreement would be subject to the internal business practices of both parties.

B. Therefore, applicable terms that should be contained within the agreement or the actual structure of the agreement are beyond the scope of this accreditation. However, both parties must recognize the benefits of preparing for the arrival of the candidate organization's CIRA Team by identifying and addressing key data elements for delivering successful CIRA services.

2.1 Elements of a CIRA Services Agreement

A. ***Capability:*** The candidate organization must include processes and procedures that, when followed, would develop an acceptable CIRA Services Agreement between the candidate organization and its clients to deliver high-quality CIRA services.

B. ***Potential Documentation Content:*** This capability is usually associated with an organization's sales or contracts department. The processes and procedures relating to developing a CIRA Services Agreement may include the following:

1. A description of the incident to the fullest extent possible.
2. The identification of the affected system(s) that are either known or believed to be associated with the incident.
3. The identification of the owner(s) of the system(s) identified in the agreement.
4. The identification of the type of CIRA services that are to be provided based on the information available.
5. A written statement from the **system owner**[9] or authorized representative, giving permission to perform the work identified in the scope document.
6. The identification of constraints on the collection and analysis of data and data content, if any. This is intended to address regulatory restrictions or capabilities that must be met.
7. The identification of the expected outcome(s) of the CIRA services that will be delivered including any deliverable items, services (e.g. malware identification, remediation or remediation assistance, etc.), products and/or reports. These items could include interim and final reports, data samples, samples of malware obtained during the investigative process, or the creation of new malware signatures.
8. The expected period of performance.
9. Estimated numbers of CIRA Team personnel who will need client facility access to meet the expected outcomes and end item deliverables within the expected period of performance.
10. A request that client technical resources, familiar with the affected system(s), be available to the CIRA Team to support the engagement.
11. A request that the clients' executive management be appropriately engaged, prior to and during the service delivery phase of the engagement, to ensure that applicable regulatory requirements are met.

[9] **Note:** For Government clients, the process should recognize that the system owner may not be the same individual as the client's contracting representative (e.g., contracting officer, contracts specialist, buyer, etc.) so the need to obtain alignment between these two responsible Government parties should be recognized within the process.

12. A suggested outline of the agreement modification process needed to address changes that may occur during the evolution of the CIRA services being provided.

C. Examples of templates for creating a Services Agreement or redacted copies of previous or existing agreements between the candidate organization and the client will meet the submission requirements associated with this section.

D. Managed Security Services or Internal Incident Response services are not within the scope of this accreditation. Sample or representative agreements that reflect this type of incident response business model are not acceptable for meeting this capability.

2.2 Client Engagement Management

A. ***Capability:*** The candidate organization must include processes and procedures that identify their approach to engage the client to fulfill the CIRA Services Agreement.

B. ***Potential Documentation Content:*** These standard client engagement management templates would be customized to support the capabilities in each specific CIRA Service Agreement. This ensures that the candidate organization's performance under each agreement is of good quality, is repeatable, and is effective. NSA/IAD recognizes that CIRA services are often provided on very short notice. It is expected that the engagement lead (Key Team Member Lead) be knowledgeable on how these processes are performed to support the needs of the client and to ensure that the organization's interests are recognized and protected. Client engagement management templates that identify minimum activities or checklists that should be performed or followed by the engagement lead could meet the intent of this requirement.

C. These processes and procedures could include:

1. CIRA Services Agreement Management
2. Coordinating an in-brief and subsequent status meetings
3. Scope confirmation and management during the course of the engagement
4. Staff and resource management
5. Technical solution management
6. Schedule monitoring and management
7. Status reporting
8. Deliverable reporting and submittals
9. Deconfliction support within the scope of their CIRA Services Agreement

D. In this context, deconfliction describes the process where the incident responder coordinates its investigative activities with the client, and through the client, with other Government organizations (i.e., DOD, law enforcement, etc.). The intent of this coordination is to ensure that its investigative activities do not interfere with another Government organization's activities. The circumstances under which the initiation of a deconfliction activity may be warranted will vary greatly and may require significant discretion and coordination to avoid disrupting other organizations' activities. Therefore, it is incumbent upon the candidate organization to recognize

that this may occur, they must be able to work through appropriate channels with its client, and they must represent how they will manage this activity.

2.3 Communication Management

A. ***Capability:*** The candidate organization must include processes and procedures that facilitate initial and on-going communications between the CIRA Team and the client.

B. ***Potential Documentation Content:*** These processes and procedures should include practices to ensure that effective communication is maintained between parties, and to ensure that appropriate operational security is practiced during those communications. These activities could include:

1. Identifying the primary points of contact for each party to the agreement, and when contacts should occur.
2. Identifying the communication channels with the system owner(s), the primary POCs, and the CIRA Team, once they arrive on site.
3. Identifying the appropriate levels of operational security (OPSEC) that should be followed when communicating between parties. This focus area could include the:
    a. Use of out-of-band communications methods for communication between parties.
    b. Prohibition of the storage of messages, incident records, copies of scans, vulnerability data or analytics on the compromised network.
4. Identifying events or activities that require the notification of the other party. For the CIRA Team these could include:
    a. Identifying any planned configuration changes to the affected system(s), such as modifying or adding applications, changing existing Access Control Lists, changing the system's availability status, etc.
    b. Notifying the involved parties that contact personnel have changed.
    c. Identifying newly discovered incidents, compromises or changes in the status of the known compromises.

2.4 Preliminary Data Collection

A. ***Capability 1:*** The candidate organization must include processes and procedures to request that, for the affected system(s), the client provides its security and system architectures for review and analysis.

B. ***Potential Documentation Content:*** This client provided data that could be used to facilitate engagement efficiency prior to the arrival of the CIRA Team. It is anticipated that such information will be needed to assess the client's implementation of defensive controls and to identify possible attack vectors across the systems attack surface. This information will assist in engagement planning purposes and would normally be needed to facilitate the preparation of recommendations at later phases of the engagement.

C. ***Capability 2:*** The candidate organization must include processes and procedures to request that the client collect incident-related information that could be used to facilitate the engagement efficiency prior to the arrival of the CIRA Team. This should include requests to turn on or deploy Intrusion Detection mechanisms as available.

D. ***Potential Documentation Content:*** The client should be requested to conduct specific and appropriate incident-related intrusion detection data collection activities before the CIRA Team arrives at the client's site. The candidate organization should also recognize industry-specific constraints or other specialized data management and protection capabilities that may impact the client's ability to perform data collection and the subsequent analysis of the collected data or the distribution of that collected data to the CIRA Team.

E. The scope of these activities will vary with the type of incident being addressed. Methodologies identified within the process should include direction to work with the client to conduct a preliminary assessment of the incident, attempt to identify system areas where preliminary data collection could be useful, and explain how that data could be used.

F. Examples of preliminary data collection could include basic intrusion detection data collection, such as turning on logging and collecting logs from the affected systems, monitoring network traffic across different protocols, deploying sniffers, and collecting system and network configurations and diagrams.

2.5 Engagement Tools and Resources

A. ***Capability 1:*** The candidate organization must include processes and procedures to ensure that the CIRA Team exercises appropriate engagement-specific planning prior to initiating work on the client's systems or system environment. This includes assigning the appropriate staff for each engagement, identifying and updating any needed tools and/or processing technology, and ensuring that sufficient processing capacity will be deployed to meet expected data processing requirements.

B. ***Potential Documentation Content:*** The processes and procedures needed to support this activity should include:

1. How the CIRA Team is composed (e.g., leadership, technical skill mix, IT expertise, etc.) based on agreement content and client needs assessments.
2. Characterizing incidents (e.g., exploit type, characteristics, etc.) obtained from client discussions, scope documents and data as available.
3. Collecting appropriate intelligence/indicator information from sources (open source, Department of Homeland Security(DHS), Information Sharing and Analysis Centers (ISACs), FBI, National Cyber Investigative Joint Task Force (NCIJTF), etc.) that will be used in the assessment. This must include acquiring pertinent, known threat intelligence from credible resources.
4. Collecting or developing client signatures or other detection methods if needed.
5. Collecting, updating, and obtaining tools expected to be used by the CIRA Team for the engagement.

C. ***Capability 2:*** When preliminary data is collected, these processes and procedures must include the performance of analysis on that collected data to determine engagement-specific needs.

D. ***Potential Documentation Content:*** The analysis of the data should be consistent with the candidate organization's normal analytical methodologies. The use of certain methods, tools,

and specific approaches should be identified. The uses of manual and/or automatic methods are acceptable approaches for analyzing collected data.

2.6 Travel Management

A. ***Capability:*** The candidate organization must include processes and procedures that facilitate the CIRA Team's rapid deployment to destinations identified in the CIRA Services Agreement. This should include, as necessary, central coordination of travel arrangements and staging and shipping of tools and IT resources needed to arrive at the client's site(s) in a timely manner.

B. ***Potential Documentation Content:*** When time is of the essence, the candidate organization should have processes in place to ensure that the CIRA Team can rapidly deploy to client sites with minimal travel delays. Processes should include travel reservations and other activities that should be completed to avoid unnecessary travel impacts or delays. For international travel, these processes should include briefing the team about destination travel alerts and providing guidance to mitigate travel risks. These could include processes to ensure that exports of software, incident response tools and systems, and other data collection tools are appropriately documented so that avoidable customs delays do not occur.

2.7 Rules of Engagement

A. ***Capability:*** The candidate organization must include processes and procedures to ensure that the CIRA Team is briefed and fully cognizant of the candidate organization's normal engagement process and are aware of any specific engagement restrictions and/or capabilities before beginning work at the client's site or accessing the client's systems.

B. ***Potential Documentation Content:*** It is expected that these processes and procedures should include:

1. What is allowed/not allowed under the CIRA Services Agreement and is part of the candidate organization's standard operating procedures
2. Current scope of work
3. Requested levels of system(s) access
4. Known damage assessment and containment capabilities
5. Data collection and analysis constraints, if any
6. Collected data protection based on client or industry capabilities
7. Incident response communication in accordance with the organization's policy
8. Points of contact and communication channels between the client and the CIRA Team
9. Planned use of collection tools and other Team resources (analytical facilities, remote access systems, etc.)

3 Incident Identification, Intrusion Detection, and Analysis (Investigation)

A. The candidate organization must include processes and procedures that recognize system-specific capabilities and the technical expertise required to collect and analyze data and to operate the associated data processing capabilities to facilitate:

1. Log collection and analysis in a wide variety of client environments. This must include all automated error reporting including reports generated by Windows systems.

2. Network traffic and flow data collection and analysis in a wide variety of client environments using both IPv4 and IPv6. This must include network device integrity checking.
3. Host integrity data collection and analysis. This must include UNIX/LINUX/MAC/Windows Operating Systems.
4. System environmental scanning for indicators of compromise.
5. Incident analysis including drive and storage forensics and malware analysis.

B. It is required that all of these activities be primarily performed on site, though NSA/IAD recognizes that supplemental support services may need to be performed at the candidate organization's facility. Specific capabilities are identified in the following sections.

3.1 Log Collection and Analysis

A. ***Capability 1:*** Within their processes and procedures, the candidate organization must include its methods and approaches to address log collection and analysis.

B. ***Potential Documentation Content:*** The processes and procedures should include standard approaches to identifying log sources using all appropriate data from all possible sources. This may include making requests to turn on logging, initiating log collection and aggregation and, to the extent appropriate, addressing log data structure normalization and filtering.

C. Contact with software vendors regarding suspicious activity may be warranted to understand the significance of vendor specific log entries or known false positives for certain intrusion detection signatures.

D. These processes and procedures should identify methods to provide adequate assurance that the integrity and confidentiality of the logs are maintained through the collection process. This would include protection approaches that could be applied during collection, transport, use, and storage. In most cases, the log collection initiation, transport, and aggregation capabilities depend on the log source and the engagement environment.

E. The candidate organization's processes should recognize how the collection, log reduction, and correlation of data found in various logs, including those obtained from security devices and systems, are normally performed.

F. In the event that the CIRA Team utilizes tools to support log data aggregation and analysis, attention should be paid to its use, ingest sizing, and any needed supporting infrastructure that will be used to perform those activities.

G. Analytical processes and procedures should identify methods using automated tools and include performing manual analysis of the collected logs. The goal could include identifying:

1. Heuristic detection when baselines are available
2. Anomalous behavior detection for networks and connected systems
3. Known malicious patterns
4. Malicious code behaviors
5. Anomalous events that require further investigations

H. ***Capability 2:*** The candidate organization must include processes and procedures to engage the client's technical resources, when needed, to obtain the required data.

I. ***Potential Documentation Content:*** The intent of this activity is to ensure that formal communication for assistance is made should client resources be required to collect or transport logs for analytical purposes.

J. ***Capability 3:*** The candidate organization must include processes to assess the system risk posture based on the log analysis and report those findings to the client.

K. ***Potential Documentation Content:*** Log analysis may result in identifying significant, new or escalating risks to the affected system or systems. The processes and procedures should clearly identify the approaches that the CIRA Team would normally take to report those identified or potential changes in the system's overall risk posture. This would include identifying the threat or exploit, what is affected, and when it occurred.

3.2 Network Traffic Data Collection and Analysis

A. ***Capability 1:*** The candidate organization must include processes and procedures to collect internet protocol derived network traffic.

B. ***Potential Documentation Content:*** This may include collecting traffic data as it crosses the client's external and internal boundaries, as well as traffic between nodes and systems on the network Virtual Local Area Networks (VLANs). This would include networks capable of running either IPv4 and/or IPv6.

C. These processes and procedures should include methods to identify network traffic collection points, data transport from those collection points, and the application or configuration of collection filters.

D. These processes and procedures should also identify methods to ensure that the integrity and confidentiality of the collected traffic data are maintained through the collection process. This includes protection approaches that could be applied during collection, transport, use and storage. In most cases the traffic data collection initiation, transport and aggregation capabilities depend on the collection point and the engagement environment.

E. ***Capability 2:*** The candidate organization must include processes and procedures to analyze network IPv4 and IPv6 traffic.

F. ***Potential Documentation Content:*** Analytical processes and procedures should identify methods to distinguish between normal traffic and traffic behavior with abnormal behaviors (unauthorized or undocumented encrypted traffic) and non-standard connections. It should include the use of automated tools and manual procedures used to analyze the data. The analytical processes should identify the candidate organization's approaches to performing:

1. Heuristic detection when baselines are available
2. Identification of malicious patterns or behaviors associated with network traffic

G. Data content analysis should be performed in accordance with the CIRA Services Agreement and should be subject to the data collection and analysis constraints identified therein.

H. ***Capability 3:*** The candidate organization must include processes to engage the client's technical resources, when needed, to obtain the required data.

I. ***Potential Documentation Content:*** In many cases, the CIRA Team will not have direct access to the systems or applications that are generating the data required for analytical purposes. Therefore, the CIRA Team should formally engage the client's technical resources to obtain that requested data. The CIRA Team should be provided with guidance or reminders that coordinating with the client's technical resources is the preferred data collection process. References to the engagement specific communication plan may be sufficient to meet this requirement.

J. ***Capability 4:*** The candidate organization must include processes to assess the system risk posture based on the network traffic analysis and report those findings to the client.

K. ***Potential Documentation Content:*** Network data analysis may result in identifying significant, new or escalating risks to the affected system or systems. The processes and procedures should clearly identify the approaches that the CIRA Team would normally use to report those identified or potential changes in the system's overall risk posture. This would include identifying the threat or exploit, what is affected, and when it occurred.

3.3 Host Integrity Data Collection and Analysis

A. ***Capability 1:*** The candidate organization's processes and procedures must recognize system-specific capabilities, technical expertise required, and data processing capabilities to facilitate host integrity data collection in a wide variety of client environments.

B. ***Potential Documentation Content:*** The candidate organization must include processes and procedures to collect and analyze the integrity of multiple types of host platforms and platform configurations. This should include UNIX/LINUX/MAC/Windows Operating Systems, system device internal operating systems and the integrity of applications that run on those operating systems. These documents could include generic data collection methods for various operating systems, applications, and purpose-built solutions that run on different classes of systems.

C. The processes should include collection tool maintenance and updating prior to use. As appropriate, this could include, acquiring and updating the tool with known threat intelligence into its analytical processes. It should also include applying appropriate security controls surrounding the system that would apply to data transport and protecting the system from malware or other security threats associated with traffic data ingest.

D. It is reasonable to anticipate that many clients will use different types of system monitoring and configuration management solutions to manage their end point hosts and network infrastructure. The engagement of client technical staff and a process to develop how those resources could be used may be appropriate.

E. The candidate organization's processes should recognize how the collection and correlation of data found within the host, including data found within integrity or configuration logs, could be collected as integrity status indicators as part of the analytical process.

F. If the CIRA Team is providing a tool or set of tools to support data aggregation and analysis, such as when automated tools are used to check the configurations of many systems, attention should be paid to appropriately sizing the tool and the supporting infrastructure to accommodate the expected volumes of data.

G. Analytical processes and procedures should identify methods using automated tools and performing manual analysis of the collected data. The goal could include identifying:

1. Binaries installed or added to the system
2. Memory dumps
3. Registry and configuration settings
4. Anomalous behavior detection for networks and systems
5. Known malicious patterns and malicious code behaviors

H. ***Capability 2:*** The candidate organization's processes and procedures must identify system-specific capabilities (e.g., Windows Workstations, Windows Servers, UNIX, LINUX, MacOS, Cisco IOS, etc.) to facilitate host operating systems and installed application integrity analysis in a wide variety of client environments. This would include listing specific tools and methods used for this purpose.

I. ***Potential Documentation Content:*** Analytical processes and procedures should identify technical expertise needed, data collection capabilities, and methods to identify apparent and probable violations of host integrity policy. It should include using automated tools and manually performing procedures to analyze the data.

J. ***Capability 3:*** Within the scope of its business model and the services that it offers, the candidate organization's processes and procedures must identify how it collects forensic evidence and how it manages that evidence to meet the legal chain of custody capabilities and related activities.

K. ***Potential Documentation Content:*** In some cases, the CIRA Team may receive data or system components, such as hard drives, with client expectations that the Team will conduct a formal forensic investigation on the received items. A chain of custody process ensures that should evidence of criminal activity be identified (e.g. security violations of an insider threat, domestic hacking, etc.) during the forensic process, the CIRA Team's client will be able to prosecute the perpetrators of the criminal activity. Conversely, this requirement is intended to preclude the CIRA Team from liability should its client intend to prosecute, but be unable to, due to a compromised chain of custody. The processes and procedures should recognize these possible consequences and provide guidance to ensure that the analysis is performed while meeting these objectives.

L. ***Capability 4:*** The candidate organization must include processes to engage the client's technical resources, when needed, to obtain the required data.

M. ***Potential Documentation Content:*** In many cases, the CIRA Team will not have direct access to the systems or applications that are generating the data required for analytical purposes. Therefore, it is incumbent upon the CIRA Team to formally engage the client's technical resources to obtain that requested data. The CIRA Team should be provided with guidance or reminders that coordination with the client's technical resources is the preferred data collection process. References to the engagement-specific communication plan may be sufficient to meet this requirement.

N. ***Capability 5:*** The candidate organization must include processes to assess the system risk posture based on the host integrity analysis performed and report those findings to the client.

O. ***Potential Documentation Content:*** Host integrity analysis may result in identifying significant, new or escalating risks to the affected system(s). The processes and procedures should clearly identify the approaches that the CIRA Team would normally take to report those identified or potential changes in the system's overall risk posture. This would include identifying the threat or exploit, what is affected, and when it occurred.

3.4 Incident Analysis

A. ***Capability 1:*** The candidate organization's processes and procedures must recognize and address the unique capabilities of analyzing sets of like data and divergent data, and then correlate that data to identify indicators and evidence of client security policy violations.

B. ***Potential Documentation Content:*** Incident analysis can be performed using a broad approach of considering log, network traffic and host integrity data and information. It may be performed using data and information that is collected incrementally from each of these data sources and then correlated to identify the apparent root cause of a particular incident where these incremental findings may meet the intent and purpose of the agreement between the client and the providers.

C. To increase the certainty that no other incident or policy violation exists beyond what may have been found through the incremental analysis, it may be necessary to perform a thorough investigation of each of these sources of data and information. Once detailed and complete data is collected, the performance of a comprehensive data analysis could be performed. Clients control the scope of work and level of effort to be delivered by the CIRA provider through the scope of the negotiated agreements. CIRA providers should have processes and procedures to reflect their business model as it may apply to either of these possible approaches.

D. The intent of this requirement is for the candidate organization to include processes and procedures that specify what the team should consider to normalize divergent data sets (e.g., correlating data from a highly customized relational database management system, from a security appliance protecting that system, and network traffic data to that system), to facilitate data ingest into an event correlation engine and then to perform analysis in accordance with their business model and service offering. If specific event correlation tools are used, these should be identified within the application package.

E. ***Capability 2:*** The candidate organization must include processes and procedures to identify and assign technical experts to perform different types of data aggregation, analysis and to use the specific processing systems and tools to perform each type of analysis.

F. ***Potential Documentation Content:*** Analytical processes and procedures vary with the type of data to be collected and the type of methods to process the data. The results of the analysis will need to be interpreted to identify apparent, probable and likely violations based on a combination of data and information from log, network traffic, and host data collected during the investigative process. Analytic methods should include the use of automated tools, as well as performing the analysis manually.

G. ***Capability 3:*** The candidate organization must include processes and procedures to use all reasonable data sources within its analytical processes.

H. ***Potential Documentation Content:*** This includes using data that are considered viable, of high integrity, this is readily available and that can be repeatedly generated ensuring the ability to perform like comparisons when needed. The intent is to ensure that all sources of data are identified, reviewed and not arbitrarily discounted or discarded by the team. Using a team approach to review multiple data sources may help yield the desired analytical outcomes.

I. ***Capability 4:*** The candidate organization must include processes and procedures to use forensic investigative techniques.

J. ***Potential Documentation Content:*** Forensics is usually performed on various systems, components, and data at some point in the incident analysis process. This includes using automated tools to collect data on incident related artifacts and to assist in the development of damage assessment. The performance of forensic based analysis may be accomplished through simple log data aggregation or through more complex memory cache-dump tools. The intent in this requirement is for the candidate organization to identify how it performs forensic analysis as part of their overall incident analysis capabilities.

K. If the candidate organization performs basic forensics internally and engages specialized organizations or support firms to provide specialized support, which is acceptable to NSA/IAD, then such approaches to providing this capability should be presented in this process and procedure. However, NSA/IAD expects that such support agreements would be established in advance. Evidence of those agreements should include identifying the subcontractor or partner organization and describing the scope of the agreements within the application package. In such cases, care should be taken to ensure that such arrangements do not conflict with the terms of the client agreement (e.g. permission to subcontract, etc.). An accreditation of the candidate organization does not imply or bestow that same accreditation to the subcontractor or partner.

L. ***Capability 5:*** The candidate organization must include processes and procedures to assess the collected analytical work and report its assessment results to the client, customer, or other parties identified in the CIRA Services Agreement.

M. ***Potential Documentation Content:*** The intent is that the candidate organization identifies how it consistently synthesizes all incident analysis work performed and assembles it into a consistent report. This would include taking automated data collection reports, event correlation reports, and manually processed data and combining it into a concise, actionable report for the client in accordance with the terms of the agreement. The reformatting and processing of tool generated reports without the application of candidate organization's staff engineering expertise is not acceptable.

N. ***Capability 6:*** The candidate organization must include processes and procedures that provide methods to assess how the technical degradations of the impacted system(s) occurred.

O. ***Potential Documentation Content:*** The selection and identification approaches should be discussed in these documents to identify variables such as attack vectors, system vulnerabilities, exploits, exploit methods, and attacker effectiveness. Furthermore, control insufficiency should be considered in the analytical approach and be reflected in the thoroughness of the resulting findings.

P. ***Capability 7:*** The candidate organization must include processes and procedures that contain methods to perform a damage assessment.

Q. ***Potential Documentation Content:*** Damage assessments require some form of valuation of the impacted systems and the data and information that they contain. The processes and procedures associated with the damage assessment should identify methods to ascertain the impacted system's value, the value of the integrity, confidentiality and availability of the data and information it contains, and how the incident affected the client. The damage assessment is the basis for the remediation recommendations and should, therefore, be diligently performed. The processes and procedures should include appropriate levels of client engagement to perform this work.

4 Containment and Remediation Recommendations

A. ***Capability 1:*** The candidate organization's processes and procedures must include a description of its standard approach to providing incident containment recommendations to the client.

B. ***Potential Documentation Content:*** All containment activities should be provided in accordance with the terms contained in the CIRA Services Agreement. The intent of this requirement is that the candidate organization should be able to provide recommendations to contain an incident/compromise. Recommendations should include the identification of all aspects of the incident or compromise, approaches to monitoring the environment and associated interconnections, and recommended actions to limit the damage or impact of the incident or compromise.

C. The accreditation program is limited to requiring that the candidate organization provide recommendations to a client's technical staff. The general methodologies for recommending containment actions for most incidents would be repeatable to a certain point, and therefore, the candidate organization's standard approach should be documented.

D. Recommendations to client management should include applying appropriate system isolation actions, tailoring countermeasures, identifying the expected duration to implement the monitoring recommendations, and interim support plans that may be required.

E. ***Capability 2:*** The candidate organization's processes and procedures must include a description of its standard approach to providing incident eradication, remediation and subsequent incident mitigation recommendations to the client.

F. ***Potential Documentation Content:*** All eradication, remediation and incident mitigation activities should be provided in accordance with the terms contained in the CIRA Services Agreement. The intent of this requirement is that the candidate organization should be able to provide recommendations to provide remediation of the incident.

G. Eradication/remediation may be considered to be a scalable activity based on system value and type of incident or intrusion detected. Conceptually, eradication could involve the use of a virus removal tool or could be significantly more involved to include isolating the infected system, performing a controlled shut down, performing low level system formats to drives, flashing the bios and rebuilding the system using new credentials and implementing other short term mitigations. Policies and procedures should be situation dependent and structured to include such an approach and recommendations as needed.

H. Mitigation is considered to be a long-term approach that is intended to reduce the likelihood of the recurrence of the same or similar instance. The candidate organization's policies and procedures may be structured to include recommending enhancements to existing controls, improvements to the systems incident detection capabilities and tuning the existing intrusion detection systems to identify and mitigate attempts to re-create the incident using the same attack vector.

I. The accreditation program is limited to requiring that the candidate organization provide recommendations, in writing, to a client's technical staff. Though direct remediation of affected systems is possible under an agreement, that level of activity is considered to be outside the scope of the accreditation program. The general methodologies for recommending containment and remediation for most incidents would be repeatable to a certain point and therefore, the candidate organization's standard approach should be documented.

J. Recommendations to client management should include applying appropriate system isolation actions, tailoring countermeasures, identifying the expected duration to implement the recommendations, and interim support plans that may be required. The documentation should identify the methods used to confirm containment, measure the progress of the remediation effort (e.g., system or service restoration, cloud reconstitution, restoration schedule, resources/budget and restoration of services, etc.), update the damage assessment (if needed), and identify any additional corrective and preventive actions to the system owners.

K. ***Capability 3:*** The candidate organization's processes and procedures must include methods to perform incident source attribution.

L. ***Potential Documentation Content:*** The intent for this requirement is that the candidate organization would use its resources in an attempt to attribute an incident to a source using all appropriate resources. The policies and procedures provided should describe methodologies that go beyond tool generated attribution reports (e.g., attacking IP, phishing scheme, web exploit, user error, etc.) and address subsequent investigation approaches that could be used to achieve this objective. This includes using the appropriate intelligence/indicator information collected as part of the pre-engagement planning identified in section 1.5 of this guide.

M. ***Capability 4:*** The candidate organization's processes and procedures must include methods to identify the status and duration of the incident.

N. ***Potential Documentation Content:*** The candidate organization would use its resources to thoroughly understand and document the status of the incident. Then, using existing data, the candidate organization would determine the status and duration (e.g., incident is concluded and remediation is required, incident is on-going and containment is required, incident is on-going but intermittent and requires both containment and remediation services, etc.).

O. A key concern is determining if the incident is concluded and that interim and final remediation plans can be identified, developed, and executed with a reasonable assurance that the same incident on the same systems will not resurface in the immediate future. The general processes that are repeatable for all types of incidents should be documented and the activities needed to support the needs of specific systems may be supplemented by the appropriate technical resources as appropriate.

P. ***Capability 5:*** The candidate organization must include processes and procedures containing methods to incorporate identified technical degradations and/or damage assessment into its remediation recommendations.

Q. ***Potential Documentation Content:*** The intent is that the candidate organization will use a formal, repeatable approach to developing remediation recommendations that are not based solely on technical recommendations intended to mitigate or eliminate the threat but include an understanding and recognition of the system owner's .

5 Post-Incident Analysis and Final Report

A. ***Capability 1:*** The candidate organization's processes and procedures must be designed to provide a post-incident information report (final report) to the client that is incident, system and NSS client specific.

B. ***Potential Documentation Content:*** Processes to facilitate post-incident analysis should reflect a level of flexibility to encompass a wide variety of clients, systems, and incident types while still establishing a repeatable and effective process.

C. Documentation should include reporting methods and approaches that fully brief the clients about the incident. Final reports should include extensive details. This should include the reconstruction of the incident timelines and specific, detailed events that formed the overall incident.

D. This process to develop the final report may include, but is not limited to, the following:

1. Assembling the CIRA Team including client incident responders, administrators, managers, and end users that were affected by the incident
2. Documenting the event by:
    a. Identifying the details of the incident in sequential order
    b. Associating a time line with the incident
    c. Identifying any sequential or cascading components of the incident
    d. Identifying the specific attack vector used and the specific vulnerability exploited at each stage of the incident
    e. Establishing the root cause of the incident

E. The final report would normally be expected to be provided in both a written form and summarized in a presentation. NSA/IAD is focused on the conveyance of effective information and recommendations to NSS owners and operators as a key part of the CIRA program. It is expected that it would include the identification of endemic system or security architecture weaknesses and provide recommended corrective actions. The process and procedure must provide recommended and tailored countermeasures for the specific system or system component designed to prevent a reoccurrence of the incident. This must include recommendations for intrusion detection enhancements or modifications (e.g., changes in the log review process, tuning of existing technical controls, new technical controls, etc.).

6 Lessons Learned

A. ***Capability 1:*** The candidate organization's processes and procedures must identify how they conduct an internal "Lessons Learned" at the conclusion of each CIRA service engagement.

B. ***Potential Documentation Content:*** The intent is to identify the strengths and weaknesses of the CIRA Team's response as well as to identify opportunities for approaching incident response engagements more effectively in the future. It is also intended to identify new or evolving operational threats that should be included in planning for future engagements.

C. The candidate organization's processes should include methods to associate the incident analysis data collection with the specific actions or inactions performed by the CIRA Team and the associated end of those specific actions or inactions results. The processes may include:

1. Assembling a CIRA Team, as well as, internal administrators and managers who participated in the cyber incident response activities.
2. When available, utilizing client input as received through comments, Situation Reports (SITREPS), feedback, and after-action reports regarding any aspect of the CIRA Team's performance should be utilized.
3. Identifying positive actions performed by users, analysts, and management, and what actions resulted in less-than optimal outcomes.
4. Documenting the timing sequences between responses and results.
5. Identifying what the staff and management would do differently the next time a similar incident occurs.

6. Reviewing the suitability of the tools that were used, identifying tools that are needed, or that need to be updated.
7. Considering the adequacy of staff training and determining if it is sufficient in providing the CIRA Team with the needed skills to address both existing and emerging threats.
8. Documenting the outcomes and incorporating them into incident response procedures, testing/exercises, and the CIRA Team training process.
9. Identifying non-process or procedure-related problems that occurred and identify corrective actions.
10. Identifying the effectiveness of the process and procedures and, should deficiencies be identified, develop corrective action plans to resolve those issues.

Appendix B – CIRA Key Team Qualifications Guide

1 Introduction

A. The **NSA/IAD Cyber Incident Response Assistance (CIRA)** accreditation is provided to organizations that have one or more CIRA Teams that are capable of delivering high quality CIRA services. NSA/IAD expects that the candidate organization's CIRA Team be structured to:

1. Meet the capabilities of the candidate organization's business model
2. Meet the demands of its clients
3. Deliver the CIRA services the candidate organization has documented in its internal policies and procedures

B. The candidate organization's Key Team Members are to be included in the application package in a format consistent with that shown in the table identified within this manual in Appendix C, Section 3 **CIRA Key Team Qualifications Report.**

C. It is critically important that individuals delivering CIRA services to NSS owners have sufficient skills to perform the work described in their employer's, the candidate organization, processes and procedures.

D. It is expected that each candidate organization will utilize at least one "Core Team" as part of its overall CIRA service offering. Each core team must consist of at least five different Key Team Members. The candidate organization represents, with the submittal of its application package, that the skills of five different Key Team Members identified and listed in **Appendix C, Section 3 - CIRA Key Team Qualifications Report,** meet the specialized expertise requirements for each Key Team Member Specialization as shown in **Table 3: CIRA Key Team Qualifications Guidance**.

E. The "skills and capabilities" represented by the industry certifications in Table 4 were identified as representing individuals who possess the key skills to meet the unique needs of CIRA service delivery. The NSA/IAD recognizes the skills associated with many of these certifications overlap and that the skills of personnel holding certifications can vary significantly. This is why certifications alone are not acceptable to meet accreditation capabilities.

F. The certifications identified are either recognized by the DOD or by members of the incident response community. DOD recognition is substantiated in DOD Manual 8570.01- updated 03/29/2013 as shown in Table 4: DOD Approved Baseline Certifications.

G. The suppliers of all certifications in Table 4 are identified in Table 5: Accreditation Reference Table. Industry certifications are not required to establish the capabilities of the five Key Team Members. However, NSA/IAD expects that emphasis will be placed on each individual's skills/education and/or experience for those who do not hold certifications to ensure compliance with Table 4. The accreditation requirement that Key Team Member abilities be

represented in the application package applies to both Government and non-Government organizations.

H. The NSA/IAD's expected capabilities for CIRA Team staffing representations are as follows:

1. The candidate organization must have its CIRA Team(s) staffed with at least five (5) different qualified individuals whose primary job functions are identified in Table 3: CIRA Key Team Qualifications Guidance.
   a. This means that there must be a different qualified individual available for assignment to a CIRA Team for each job title identified in the table.
   b. Additional technical or administrative personnel may be appropriately assigned to the CIRA Team who possess technical Original Equipment Manufacturer (OEM) certifications not identified within the table (e.g., Microsoft Certified Systems Engineer (MCSE), Cisco Certified Internetworking Engineer (CCIE), etc.), but those individuals do not count towards meeting the accreditation staffing expectations.
   c. Alternative certifications for Security Management, Security, Incident Response, and Forensic may be proposed and will be considered as part of the staffing evaluation process.
   d. Part time contactors, subcontractors and other resources **may be part** of the organization's CIRA Team. However, any individual certifications and qualifications from other organizations ***may not be*** counted toward this accreditation.

Table 3: CIRA Key Team Qualifications Guidance

Key Team Member Specialization	Position Qualifications (Expansion of these elements are permissible when presented in the associated resume(s))	Expected Experience	Qualified Staff Compliance with at least one of these two columns	
			Commercial Certification (May have one of these certifications)	Individual Staff Education and Experience Levels
CIRA Team Leader	Individuals qualifying to meet the capabilities of this position must possess a thorough understanding of: • Managing Information Assurance tasks, projects or programs • Project Management, scope management and client relationship management • The candidate organization's Information Response Assistance processes • NIST/CNSS Risk Management Processes, Control Application/Test, Incident Response, Forensic and related guides • Legal/Regulatory requirements as they relate to NSS. • Basic to expert knowledge of Incident Response, Forensics, Incident Data Analysis, Network Defense and associated analytical tools • National Security Systems (NSS) management, operation and data protection capabilities • NSS Change Management Processes • Preparing and presenting final reports	Has experience in leading not less than 5 Security assessment projects in the previous two (2) years (avg. 1 every 4 months).	**Primary Certifications: CISSP-ISSMP, GSLC or CISM** **Alternative Certifications: CISSP**	Degree in management, Management Information Systems or Computer Science. MS Degree + 3 years managing Technical tasks and projects. 2 of those years Managing Information Assurance Tasks or Projects. BS Degree + 4 years managing Technical tasks and projects. 3 of those years Managing Information Assurance Tasks or Projects. No Degree + 5 years managing Technical tasks and projects. 4 of those years Managing Information Assurance Tasks or Projects. No Degree + 3 years managing Technical tasks and projects as a U.S. Government-employed Incident Response Team lead.
Incident Responder	Individuals qualifying to meet the capabilities of this position must possess a thorough understanding of: • Delivering Incident Response Assistance services as an Incident Responder • NIST/CNSS Risk Management Processes, Control Application/Test, Incident Response, Forensic and related guides • Legal Capabilities as they relate to NSS	Should have experience in supporting not less than 6 Information Security/ Incident Response projects in the previous	**Primary Certifications: GCIH, CSIH, CEH or E|CIH** **Alternative Certifications: CISSP, CASP, GPEN, CRISC, CASP**	Degree in Management Information Systems or Computer Science. MS Degree + 3 years Information Security work. 2 of those years performing Incident Response support. BS Degree + 4 years Information Security work. 3 of those years performing Incident Response support.

Key Team Member Specialization	Position Qualifications (Expansion of these elements are permissible when presented in the associated resume(s))	Expected Experience	Qualified Staff Compliance with at least one of these two columns	
			Commercial Certification (May have one of these certifications)	Individual Staff Education and Experience Levels
	• Incident Detection Techniques including the use of Vulnerability Assessment Tools • Working with Client CSIRTs • Incident categorization based on client baselines and parameters • Handling Host and Network sourced incidents • Forensic data collection • Incident Impact Assessments • Incident Containment methodologies • Change Management processes • Preparing and Presenting Findings	two (2) years (avg. 1 every 3 months).		No Degree + 5 years providing support to Technical tasks and projects. 4 of those years performing Incident Response support. No Degree + 3 years providing incident response Technical services under tasks and projects as a U.S. Government-employed Incident Response Team member.
CND Analyst (Forensics)	Individuals qualifying to meet the capabilities of this position must possess a thorough understanding of: • Delivering Incident Response Assistance services as a Forensic Analyst • NIST/CNSS Risk Management Processes, Control Application/Test, Incident Response, Forensic and related guides • Forensics as it relates to Legal/Regulatory requirements as they relate to NSS • Media Management for forensic purposes • Media Examination and analysis techniques including the use of Forensic Tools for Networks, Network components, Hosts and Host components, Software and software use • Data Recovery techniques • Analysis of Recovered Data (low and high level) • Change Management processes • Preparing and Presenting Findings	Should have experience in supporting not less than 6 Information Security/ Forensic analysis projects in the previous two (2) years (avg. 1 every 3 months).	**Primary Certifications: GCIA, CEH, GCED, CFCE, or CCE, GREM, GPEN** **Alternative Certifications: CRISC, EnCE**	Degree in Management Information Systems or Computer Science. MS Degree + 3 years Information Security work. 2 of those years performing Forensic Analysis support. BS Degree + 4 years Information Security work. 3 of those years performing Forensic Analysis support. No Degree + 5 years managing Technical tasks and projects. 4 of those years performing Forensic Analysis support. No Degree + 3 years providing CND Analytical services under tasks and projects as a U.S. Government-employed CND Analyst focusing on Forensics.

Key Team Member Specialization	Position Qualifications (Expansion of these elements are permissible when presented in the associated resume(s))	Expected Experience	Qualified Staff Compliance with at least one of these two columns	
			Commercial Certification (May have one of these certifications)	Individual Staff Education and Experience Levels
CND Analyst	Individuals qualifying to meet the capabilities of this position must possess a thorough understanding of: • Delivering Incident Response Assistance services as a Network Defender/Analyst • NIST/CNSS Risk Management Processes, Control Application/Test, Incident Response, Forensic and related guides • Legal Capabilities as they relate to NSS • Incident Detection Techniques including the use of Vulnerability Assessment Tools • Network Architectures, Microsoft Domains/Protocols and Unix network environments • Microsoft OSs, UNIX/Linux based OSs, Network IOSs and other operating systems (Mainframe, CDS, SAN Fabrics, Custom configurations, etc.) • Application operational characterization and variance detection • Incident Detection Techniques including Network data collection and message analysis • Network, host, security device and application log analysis • WEB/Mobility Log Analysis • Wireless, VoIP and POTs Log Analysis • HIDS, NIDS and Security Appliances • Firewalls and UTMs • SIEM and Event Correlation Tools and their use • Data collection management and analysis • Root kit/malware characterization and analytics • Change Management processes	Should have experience in supporting not less than 6 Information Security/CND projects in the previous two (2) years (avg. 1 every 3 months).	**Primary Certifications: GCIA, CEH, or GCED** **Alternative Certifications: CRISC, CISSP**	Degree in Management Information Systems or Computer Science. MS Degree + 3 years Information Security work. 2 of those years performing Network Defender Analysis support. BS Degree + 4 years Information Security work. 3 of those years performing Network Defender Analysis support. No Degree + 5 years managing Technical tasks and projects. 4 of those years performing Network Defender Analysis support. No Degree + 3 years providing CND Analytical services under tasks and projects as a U.S. Government - employed CND Analyst.

Key Team Member Specialization	Position Qualifications (Expansion of these elements are permissible when presented in the associated resume(s))	Expected Experience	Qualified Staff Compliance with at least one of these two columns	
			Commercial Certification (May have one of these certifications)	Individual Staff Education and Experience Levels
	• Preparing and Presenting Findings			
Auditor / Vulnerability Analyst	Individuals qualifying to meet the capabilities of this position must possess a thorough understanding of: • Delivering Incident Response Assistance services as an Information Security Auditor • NIST/CNSS Risk Management Processes, Control Application/Test, Incident Response, Forensic and related guides • Legal Capabilities as they relate to NSS • Audit Planning and data collection techniques • NSS permitted or allowed use auditing • Audit Quality Assurance Techniques • Incident Detection Techniques including the use of Vulnerability Assessment Tools • Auditing Network Architectures, Microsoft Domains/Protocols and Unix network environments • Auditing Microsoft OSs, UNIX/Linux based OSs, Network IOSs and other operating systems (Mainframe, CDS, SAN Fabrics, Custom configurations, etc.) • Auditing of databases, • Auditing WEB/Mobility Services • Auditing Applications • Supply chain security auditing • Change Management processes • Preparing and Presenting Findings	Should have experience in supporting not less than 2 Information Systems/Information Security/Information Assurance Audit projects in the previous two (2) years.	**Primary Certifications: GSNA, CEH or CISA** **Alternative Certifications: CRISC, CISSP, CISSP-ISSEP, CISSP-ISSAP**	Degree in Management Information Systems or Computer Science. MS Degree - 3 years managing Technical tasks and projects. 2 of those years Managing security assessment projects. BS Degree - 4 years managing Technical tasks and projects. 3 of those years managing security assessment projects. No Degree - 5 years managing Technical tasks and projects. 4 of those years managing security assessment projects. No Degree + 4 years providing CND Analytical services under tasks and projects as a U.S. Government-employed Information Assurance Auditor.

DOD Certification Baseline for CND activities. Reference Appendix 3 of DOD Manual 8570.01-Manual updated 01/24/2012

Table 4: DOD Approved Baseline Certifications

CNDSP Analyst	CNDSP Infrastructure Support	CNDSP Incident Responder	CNDSP Auditor	CNDSP Manager
GCIA CEH GCIH	SSCP CEH	GCIH CSIH CEH	CISA GSNA CEH	CISSP-ISSMP CISM

Table 5: Accreditation Reference Table

Accreditation Provider	Accreditation Name
International Information Systems Security Accreditations Consortium (ISC)2	Certified Information Systems Security Professional (CISSP) Certified Information Systems Security Professional –Information System Security Management Professional (CISSP-ISSMP)
System Administrator, Audit, Network, Security (SANS) Institute	GIAC Certified Incident Handler (GCIH) GIAC Certified Intrusion Analyst (GCIA) GIAC Certified Enterprise Defender (GCED) GIAC Systems and Network Auditor (GSNA) GIAC Reverse Engineering Forensics (GREN) GIAC Penetration Tester (GPEN) GIAC Security Leadership Certification (GSLC)
Carnegie Mellon University, Software Engineering Institute (CMU, SEI)	Certified Computer Incident Handler (CSIH)
Electronic Commerce Council (EC-Council)	EC-Council Certified Incident Handler (E|CIH) Certified Ethical Hacker(CEH)
The International Association of Computer Investigative Specialists (IACIS)	Certified Forensic Computer Examiner (CFCE)
The International Society of Forensic Computer Examiners (ISFCE)	Certified Computer Examiner (CCE)
Information Systems Audit and Control Association (ISACA)	Certified Information Security Auditor (CISA) Certified Information Security Manager (CISM) Certified in Risk and Information System Control (CRISC)

Appendix C – Accreditation Application Package

This appendix contains the formatted forms that a candidate organization should include when applying for accreditation. These completed forms, in addition to the supporting documentation representing a candidate organization's processes and procedures, comprise an accreditation application package.

[Remainder of the Page Intentionally Left Blank]

1 Application for Accreditation

Organization Name	
Cyber Incident Response Business Unit Address (If Applicable)	
Street Address	
City, State, Zip	
Point of Contact	
Phone Number	
Fax Number	
Email Address	
DUNS Number (if Applicable)	
Cage Code (if Applicable)	

2 Business Statement of Intent Certification

We, the undersigned, believe and in good faith attest to the following:

As part of our business model and as a normal course of business, _____ delivers its incident response services as part of a U.S. controlled business in its day to day business operations.

As authorized representatives of _____ and to the best of our knowledge, we believe that _____ and/or members of its cyber incident response staff are eligible to hold and/or maintain a U.S. Government security clearance.

To the best of our knowledge, we believe that _____ intends to maintain its cyber incident response capabilities, as represented by the information contained in this application package, for delivering Cyber Incident Response Assistance (CIRA) services through the evaluation period and for the following 24 months should an accreditation be issued.

Should _____ be granted an accreditation in CIRA Services, we acknowledge that, to remain in good standing, we will notify NSA/IAD accrediting office of any material changes to the information in the application package. Material changes could include, but are not limited to, changes in organization ownership or reporting responsibility, changes to its business focus, changes in clearance eligibility, etc. Furthermore, we acknowledge that certain changes may result in the re-evaluation of the application package and may result in the revocation or non-renewal of a previously issued accreditation.

Submitted by:

Company: _____

Authorized Official: [Signature] _____ Date:
[Printed Name/Title]

Authorized Official: [Signature] _____ Date:
[Printed Name/Title]

3 CIRA Key Team Qualifications Report *

Representative Team Member Job Title	Years' Experience	Commercial Certification(s)	Education and Experience Level Summary	Supporting Data Attached? Yes/No
CIRA Team Leader				
Incident Responder				
CND Analyst (Forensics)				
CND Analyst				
Auditor				
The information presented in this table is accurate as of: (*Insert effective date in the space to the right of sentence above.*) **The effective date must coincide within 30 calendar days of the application submittal date.**				

This table must be completed and any supporting data must be submitted as part of the candidate organization's application.

4 Application Content Checklist for a Candidate Organization

Candidate organizations are requested to complete this cross reference checklist and include it as part of this submittal.

Document Name	Capability Description	Included in the Package? (Y/N)	Cross Reference Document Name including information Location/Section/Paragraph/etc. (If Applicable).	NSA/IAD Verified
Business Statement of Intent	A formal statement signed by two executive officers of the organization asserting its commitment to perform CIRA services.		Part of the application form – Has it been signed?	
Core Capabilities Overview	Documentation that describes the core capabilities that describe how a candidate organization performs CIRA analysis.			
Processes and Procedures	Processes and procedures used to perform and deliver CIRA services.			
	Preparation and Planning			
	Services Agreement			
	Client Engagement Management Processes			
	Communication Management Processes			
	Preliminary Data Collection			
	Engagement Tools and Resources Identification			
	Travel Management Processes			
	Rules of Engagement			
	Identification, Detection, and Analysis			
	Log Collection and Analysis			
	Network Traffic Data Collection and Analysis			
	Host Integrity Data Collection and Analysis			
	Incident Analysis			
	Containment and Remediation Recommendations			
	Post-Incident Analysis			

Document Name	Capability Description	Included in the Package? (Y/N)	Cross Reference Document Name including information Location/Section/Paragraph/etc. (If Applicable).	NSA/IAD Verified
	Lessons Learned			
CIRA Key Team Qualifications Report	Documentation that describes the skills of the candidate organization's Key Team Members who will deliver CIRA services to its clients.			
CIRA Education and Training	Evidence that the candidate organization's technical and management staff are keeping up to date on current CIRA techniques.			
Past Performance	At least three (3) final reports, modified to protect the client's identity, generated at the conclusion of separate CIRA service engagements performed by the candidate organization in the previous 24 months.			
Client-Furnished Information and Data	Identifying the candidate organization's capabilities to manage customer property and information in a secure manner.			